Monday, August 30, 2004 New York Law Journal

Health Care Law

The Evolving Protections Of HIPAA Regulations

BY RONALD J. LEVINE, ANNE MALTZ AND RACHEL C. ENGELSTEIN

APRIL 14, 2003, was a much dreaded day for many health care providers. More frightening than the doomsday predictions for Y2K was HIPAA — the Health Insurance Portability and Accountability Act, whose privacy regulations became effective that day. Undoubtedly, these regulations have changed the nature of how a patient's medical information is handled and disclosed. Some of the changes have been obvious such as the cover sheet over waiting room sign-in lists; others, such as the modification to the 'legalese' on records release forms, have been less so.

A year since their implementation, this article will highlight certain key court decisions interpreting and applying HIPAA's privacy regulations and examine to what extent the government has been enforcing them. It will also explore the continuing need for self-audit by health care providers and the need to ensure that the means by which attorneys seek protected health information (PHI) conforms to the regulations. Furthermore, as we approach the deadline for compliance with HIPAA's security regulations (April 21, 2005), we discuss what additional initiatives should be undertaken.

HIPAA in the Courts

The privacy regulations create broad protections with regard to a patient's PHI and have significantly altered the means by which such information can be obtained.

The HIPAA regulations permit covered entities, which include physicians, hospitals and insurance companies, among others, to disclose PHI "in response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order."[1]

Disclosure is also permitted in response to a subpoena or written discovery request if the covered entity receives adequate assurance that the requesting party has attempted to provide written notice to the patient, or if reasonable efforts have been made to secure a protective order. Any objections raised by the patient must be resolved prior to the release of the information.[2] In the alternative, the information can be released if there is a protective order in place, either by agreement of the parties or by order of the court, that "[p]rohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding" and requires the return or destruction of the PHI at the end of the litigation or proceeding.[3]

HIPAA contains a preemption clause which provides that if a state law is less stringent, i.e. less protective of individually identifiable information, than HIPAA, the state law shall be preempted by the federal regulation.[4] Conversely, more stringent state laws are not preempted. Significantly, since the effective date of the privacy regulations, many of the HIPAA-related lawsuits have involved HIPAA's preemption provision.[5]

New York's most notable HIPAA decision, *National Abortion Federation v. Ashcroft*,[6] dealt with this very provision. The court in the Southern District of New York found that C.P.L.R. 4504(a), which prohibits a health care practitioner from disclosing PHI without express consent by the patient, to be more stringent than HIPAA because the C.P.L.R. requires patient consent and HIPAA contains certain exceptions.[7] However, the court held that the language of the preemption provision does not give more stringent state law the force of federal law. In cases where state laws would apply, it merely prevents the replacement of state law with the less stringent HIPAA provisions. In federal question cases, HIPAA provisions would not be supplanted by New York law.[8] The court also found that Rule 501 of the Federal Rules of Evidence required that the HIPAA regulations, not the privilege rules embodied in Rule 501, controlled the enforceability of subpoenas of medical records.

New York courts have also recently evaluated the force and effect of a health care proxy that was signed prior to HIPAA's implementation.[9] While HIPAA clearly necessitates a patient's consent prior to the release of his medical records, with certain limited exceptions, it does not provide much guidance in the event that the patient is not competent to provide such consent. In *Mougiannis v. North Shore*, the state Supreme Court in Nassau County looked to the patient's intent in signing the health care proxy, prior to her incapacitation, to empower her daughter to manage her health care decisions. The court found, consistent with New York Public Health Law,[10] that the validly executed health care proxy granted the daughter-petitioner the right to request her mother's medical records, in order to make informed medical decisions. Prudent attorneys, however, should

Ronald J. Levine *is a partner,* **Anne Maltz** *is counsel, and* **Rachel Engelstein** *is an associate with Herrick, Feinstein.*

advise their clients to execute a HIPAA authorization form when other planning documents are signed.

While a cursory reading of the regulations may suggest that they apply only to written requests for PHI, several courts have held otherwise. In a recent Southern District of California case, the court held that an attorney had violated HIPAA by engaging in an ex-parte conversation with the plaintiff's examining physician. The parties to the case had executed a typical protective order regarding documents and information produced by the defendant. The protective order, however, did not provide similar coverage to the plaintiff's information. Because HIPAA does not authorize ex-parte communications with physicians, the attorney should have submitted a formal discovery request, along with an authorization from the patient, in order to comply with the regulations.[11]

In a similar case, a Maryland federal court held that not all ex-parte communications with an adversary's health care practitioner were prohibited by HIPAA; conversations discussing serving a subpoena or scheduling a deposition are clearly outside the scope of the regulations. However, when the ex-parte communication leads the doctor or nurse to orally disclose PHI, the communication is then subject to HIPAA's privacy protections.[12]

Enforcement

In light of the enormous build-up to the effective date of the privacy regulations, health care providers have since been whispering the ultimate question: Is anyone really verifying my compliance? The answer is yes.

The Office of Civil Rights (OCR), a division of the Department of Health and Human Services (HHS), is charged with civil enforcement of the privacy regulations. Its mandate is to encourage voluntary compliance by covered entities and provide an opportunity to cure any deficiencies. While OCR is authorized to take an active approach to compliance by conducting audits,[13] its current approach is primarily complaint driven.[14]

According to OCR, it receives approximately 100 privacy-related complaints per week. Of the 6,500 complaints filed as of May 31, 2004, 51 percent have not been pursued by OCR due to lack of jurisdiction. Furthermore, many of the complaints were not investigated because either the alleged misconduct did not violate HIPAA or voluntary compliance by the covered entity remedied the situation. As of June 30, 2004, no civil money penalties had been levied for HIPAA violations;[15] however, 80 of the complaints have been referred to the Department of Justice for criminal investigation and possible sanction.[16]

The procedural enforcement rules that govern OCR were published on April 17, 2003, as an interim final rule, modeled after those used by HHS's Office of Inspector General.[17] Because the substantive enforcement rules have not yet been published, if OCR were to levy a monetary penalty for a violation of a privacy regulation, many HIPAA experts have speculated that such penalty would likely be challenged by the recipient as lacking the necessary statutory authority.

In light of the enormous build-up to the effective date of the privacy regulations, health care providers have since been whispering the ultimate question: Is anyone really verifying my compliance? The answer is yes.

Practical Need for Self-Audit

Seeking medical records and other PHI in the course of litigation subjects both attorneys and health care providers to HIPAA's privacy regulations. Covered entities are required by the regulations to keep audit records and compliance reports, which the Secretary of HHS can request at any time in order to verify the covered entity's compliance.[18] It is therefore important that the entity conduct routine self-audits to assure compliance with the regulations. Even though most attorneys are not subject directly to the HIPAA regulations,[19] they should, nevertheless, remain mindful of the privacy regulations in order to avoid delay in the discovery process.

Auditing compliance efforts is the only effective means to determine whether a covered entity is following the privacy regulations. Proper documentation of self-audits will also assist the defense in the event of a civil complaint. These audits can be conducted by the covered entity itself, but it is often advisable, depending on the size and complexity of the organization, to employ the services of an attorney familiar with the regulations to assist in the audit.

While in an ideal world, every aspect of the HIPAA privacy regulations would be adhered to, highlighted below are the areas most requiring scrutiny by covered entities.

Privacy Notice:

- Is the notice current? Is it consistent with the entity's operations?
- Is there a written procedure describing the delivery and retention of the privacy notice and its acknowledgement? Is the procedure followed?

Authentication:

- Is there a written procedure for verifying and authenticating all individuals and entities requesting information? Is the procedure followed?
- If a request is accompanied by a patient authorization, how is the authorization verified? Is the health care provider aware of the necessary language to constitute a valid release?
- How does the health care provider confirm that the requesting entity is entitled to receive the information? Is such confirmation documented?

Releasing Protected Health Information:

- Is there a procedure to verify that only the information requested or authorized is actually released? Is the procedure followed?
- Are copies of the requests or authorizations maintained on file?
- Is the health care provider aware that PHI may be released without authorization if the release is related to treatment, pay-

ment or health care operations? Does it know how to recognize such requests?

Complaints and Questions:

• Has a privacy officer been designated and properly trained?

• Is the privacy officer available to answer questions for staff and patients regarding the release of PHI and also to address complaints?

• How are complaints addressed and infractions remedied?

Issues for Attorneys

While not subject to the regulations themselves, attorneys seeking to obtain PHI in the course of discovery, should be mindful of the following issues.

Authorizations:

• Do the authorizations/releases by which PHI is requested comply with HIPAA?[20]

Handling Protected Health Information:

• Who within the legal team is permitted to access and examine the PHI once it is received?

• How are the records maintained in order to preserve confidentiality? Are the records adequately protected if made part of the court record or if they are shared with experts?

• Are the records adequately protected during the course of depositions or open court proceedings?

HIPAA Security Regulations

In contrast to the privacy regulations that apply to PHI in any form, HIPAA's security regulations, with a compliance deadline of April 15, 2005, apply only to PHI transmitted or maintained in electronic media. Many covered entities will be required to implement significant modifications to their daily routines and technologic systems to ensure compliance by the deadline.[21]

The purpose of the security regulations is to develop and implement a compliance program to protect electronic PHI (EPHI). Like the privacy regulations, the security standards are scalable, based upon the size, capabilities and complexity of the covered entity. The security regulations are divided into three categories: administrative, physical and technical. Provided below are examples of one requirement from each category.

The administrative standards require, for example, that each covered entity adopt policies to prevent, detect and correct security violations and designate a security official responsible for the implementation thereof.

The physical standards are intended to prevent unauthorized physical access to IT systems and facilities, while simultaneously monitoring and permitting authorized access. The physical standards also address the need to develop a disaster recovery plan to facilitate data access in the event of an emergency.

Lastly, the technical safeguards require, among other things, that each covered entity implement a system to record and examine IT activity in those systems containing EPHI.

The first step to security compliance is determining the covered entity's needs, in light of the regulations. Covered entities are advised to hire an experienced IT professional to conduct a thorough risk analysis of its computer systems to determine the necessary modifications. This evaluation should be conducted in conjunction with a knowledgeable attorney who can assist the covered entity in prioritizing the risks, as well as in implementing the new policy. As with the privacy regulations, self-audits will be necessary to ensure continuing compliance.

HIPAA Going Forward

As the general public becomes increasingly aware of the rights granted to them by both the privacy and security regulations, the number of complaints filed with OCR is likely to rise. As this happens, the OCR will most likely take a stricter stance regarding noncompliance, which could lead to civil or criminal penalties and the filing of more civil suits by private citizens. Furthermore, if the federal government remains committed to transitioning to an exclusively electronic records system, HIPAA compliance will receive even greater scrutiny.[22] For this reason, it will become progressively more important for covered entities and their business associates to routinely conduct self-audits to verify compliance with the regulations. In this evolving area of law, attorneys representing covered entities or those seeking information from covered entities must carefully monitor any pending HIPAA-related lawsuits whose decisions could alter the interpretation or implementation of the regulations.

1. 45 C.F.R. §164.512(e)(1)(i).
2. 45 C.F.R. §164.512(e)(1)(ii).
3. 45 C.F.R. §164.512(e)(1)(iv-v).
4. 45 C.F.R. §160.202.
5. 45 C.F.R. §160.203.
6. *National Abortion Federation v. Ashcroft*, 2004 U.S. Dist. Lexis 4530 (S.D.N.Y. March 19, 2004).
7. In contrast to New York law, HIPAA does permit disclosures during a judicial proceeding without authorization by the patient if certain steps are taken, as described above.
8. *National Abortion Federation v. Ashcroft*, 2004 U.S. Dist. Lexis 4530 (S.D.N.Y. March 19, 2004).
9. *Mougiannis v. North Shore-Long Island Jewish Health System*, N.Y.L.J., May 19, 2004 (Supreme Court, Nassau Co.).
10. NYPHL §18, §2982 (2003).
11. *Crenshaw v. Mony Life Insurance Co.*, 2004 U.S. Dist. LEXIS 9882, *33-39 (S.D. Calif. April 27, 2004).
12. *Law v. Zuckerman*, 307 F.Supp.2d 705, 708-10 (D. Md. 2004).
13. 45 CFR §160.308.
14. Civil Money Penalties: Procedures for Investigations, Imposition of Penalties, and Hearings, 68 Fed. Reg. 18,895 (April 17, 2003).
15. HHS's statutory authority to levy civil monetary penalties for the wrongful disclosure of PHI is found at 42 U.S.C. §1320(d)(5).
16. Jodi Goldstein Daniel, Office of General Counsel, Civil Rights Division of HHS, addressing American Health Lawyers Association (June 30, 2004).
17. See 42 C.F.R. §§1003, 1005, 1006.
18. 45 C.F.R. §160.310.
19. Only if an attorney is a "business associate" of a covered entity would s/he be subject to HIPAA. See 45 C.F.R. §160.103 for the complete definition of a business associate. Generally a "business associate" is an entity that acts on behalf of a covered entity and handles PHI.
20. The authorization form must contain nine basic elements; the requirements are discussed at 45 C.F.R. §164.508(c).
21. 45 C.F.R. §§160, 162, 164. The compliance date for small health plans is April 2006.
22. Press Release, U.S. Department of Health and Human Services, "Secretary Thompson, Seeking Faster Possible Results, Names First Health Information Technology Coordinator," May 6, 2004, (available at http://www.hhs.gov/news).